State of Montana Information Security Advisory Council
Minutes
February 8, 2017
1:00 PM
Cogswell Building, Room 151

Members Present:

Ron Baldwin CIO/SITSD, Chair
Lynne Pizzini, CISO/SITSD
Erika Billiet, City of Kalispell
Joe Frohlich, SITSD
Stuart Fuller, DPHHS
John Burrell, MATIC/Justice
Jon Straughn, COR
Jim Gietzen, OPI
Dawn Temple, DOJ, Alternate
Craig Stewart, DMA
Kreh Germaine, DNRC
Adrian Irish, UoM
Margaret Kauska, DOR

Staff Present:
Wendy Jackson

Guests Present:
Anne Dormady, Sean Rivera, Channah Wells, Cyndie Lockett, Rebecca cooper, Dawn Pizzini, Carroll Benjamin, Rennan Rieke

Real-time Communication:
Michael Jares, John Cross, Rawlin Richardson, Anne Kane, Rick Hancock, Angie Riley, Brian Jacobson, Suzi Kruger, Terry Meagher, Zac Day, Jeff Slavick, Jerry Kozak, Jerry Marks, Josh Rutledge, Kyle Belcher, Larry Krause, Lance Wetzel, Michael Barbere, Chris Silvonen, Manuel Soto, Christi Mock, Tom Murphy, Cheryl Pesta, Erin Stroop, Sky Foster, Glynis Gibson, Chris Hunt, Dwain Erhart, Mike Mazanec, Edwina Morrison

Welcome and Introductions
Lynne Pizzini welcomed the council to the February 8, 2017 Montana Information Security Advisory Council (MT-ISAC) meeting. All members and guests were introduced.

Minutes
Motion: Lynne Pizzini moved to approve the January 11, 2017 minutes as presented. Margaret Kauska seconded the motion. Motion passed.

Business
Legislative Session
Ron Baldwin reported that SITSD gave a presentation to General Government. General Government is in the process of budget reviews.
Ms. Pizzini stated there will be executive action on the DOA/SITSD budget on Tuesday, February 14, 2017.

State Continuity & Emergency Management
Dawn Pizzini gave a presentation on State Continuity and Emergency Management. She reviewed the Living Disaster Recovery Plan System (LDRPS 10) and her office's continuity plan. Dawn Pizzini stated that, due to limited state resources, there is a process that prioritizes the recovery of essential services. This process is known as the Business Impact Analysis and involves a priority rating score and a criticality rating. This score determines what priority or criticality rating a business process receives. These scores are used to determine the priority for service recovery. The recovery time objective outlines how the process can go without recovery before there are intolerable consequences to the state and assigns a numeric value based on criticality. There are seven State Essential Functions (SEFs) which align directly with the eight National Essential Functions (NEFs) of government. The SEFs are set by the federal government and standardized across all states. The process in need of recovery are measured against the SEFs to determine what, if any, affect this process has on the SEFs. The level of impact on SEFs is also assigned a numeric value. Every process in state government is evaluated through this process to determine the level of importance to state government. A Business Process Analysis, called Snapshot Report, is used to identify the dependencies that must be in place

to perform the SEFs. This involves equipment and supplies, telecommunications, physical seating, tele-work recovery, essential records, and essential information systems and software. Dawn Pizzini stated that the dependencies are inheriting their criticality from the business processes that they support. This provides vital information concerning the critical nature of each business process. NIST 800-34 (Contingency Planning Guide for Federal Information Systems) identifies various plan types that are part of contingency. This includes Information Technology Disaster Recovery, Business Continuity Plans, and Information System Contingency Plans (ISCPs). There is currently not a template available for ISCPs. A Statement of Work is being developed to migrate from LDRPS 10 to LDRPS 11, or Assurance CM. This migration will move the contingency plans from a .Net framework application to a browser agnostic environment and allow for a more user-friendly experience. The deadline for this migration is June 30, 2017. Dawn Pizzini stated that continuity management focuses on impact rather than cause of the scenario. For power outages, Emergency Action Plans (EAPs) will be followed to ensure the safe exit of employees from the affected facility. The Disaster and Emergency Leave Policy provides guidelines for determining if it is appropriate to send employees home. There is a Memorandum of Understanding (MoU) with the Helena Public School System where state employees can relocate to a public school facility if necessary. LDRPS System at Time of Event is hosted with SunGard in multiple data centers. This system is replicated on the East and West Coast. There is a 20-minute service agreement with SunGard to have access to those plans. Those plans can be accessed from any location via the internet. Continuity coordinators are responsible for establishing guarantee access to continuity plans. This may include the storage of plans in multiple locations. These plans are security documents and should be treated as such. The State of Montana also utilizes the State Emergency Notification system via SunGard. This system is available to all state agencies and allows users to push notifications to state employees. Lynne Pizzini verified that SITSD uses the SunGard State Emergency Notification system through it's ISIRT and encouraged other state agencies to establish this same type of notification for their emergency response team. This system is tested monthly to ensure it is functioning properly.

Q: Stuart Fuller: Are there any plans to produce a statewide template for ISCPs?
A: Dawn Pizzini: That would be up to the State CIO and CISO. I believe that would make sense.
Q: Mr. Fuller: HHS has three affected documents for each system. The System Security Plan, Risk Assessment, and the Authorization to Operate documentation. We would like the ability to put these documents in LDRPS 10.
A: Dawn Pizzini: Those documents could either be attached to the plan, or they could be stored as essential records.
Q: Mr. Baldwin: In the event of an emergency, how do we focus ourselves and determine the appropriate next steps and contact information?
A: Dawn Pizzini: Many of the individual departments have internal incident management teams to respond to incidents within their department. Policy writing may be necessary to fill the holes in communication that exist outside of Helena.

MT-ISAC Topics of Discussion
Data Loss Prevention
Mr. Frohlich stated that OneDrive for Business data is stored in Microsoft tenant space. Files added to OneDrive for Business are secure and encrypted both at rest and in transit. This differs from Exchange, which in most cases is unencrypted clear text sent over the internet. Data Loss Prevention (DLP) is set to notify on one instance for internally shared information on OneDrive for Business. The MT-ISAC approved DLP to block on one instance for Exchange. MT-ISAC recommends that DLP continues to notify on one instance for OneDrive for Business internal shares. External sharing on OneDrive for Business is currently not available. Dave Johnson commented that very little testing has been done with external sharing on OneDrive for Business because it has not been turned on yet. Microsoft authentication will be required for external sharing. Documents outlining how to create a Microsoft authentication will be available once external sharing has been turned on.
Mr. Frohlich requested that the council endorse turning on the template for external sharing in OneDrive for Business which will block on one instance.
Kreh Germaine stated his support for the turning on of DLP for external sharing in OneDrive for Business.

Motion: Lynne Pizzini made motion to turn on the external sharing on OneDrive for Business with a DLP template that will block on one instance of sensitive information sharing. Mr. Germaine seconded the motion.

Motion carried.

Motion: Lynne Pizzini made motion to remove the ABA routing numbers from the DLP templates for both Exchange and OneDrive for Business. Dawn Temple seconded the motion. Motion carried.

Motion: Stuart Fuller made a motion to allow Joe Frohlich, as the manager of the Enterprise Security Program, to adjust the threshold levels on the DLP templates to quickly address any issues that may arise. Dawn Temple seconded the motion. Motion passed.

Action Item: Mr. Frohlich will inform MT-ISAC of any adjustments made to the DLP template threshold levels.

Mr. Germaine emphasized the importance of timely communication regarding any changes made to the DLP template threshold levels.

Q: Mr. Fuller: What is the use case difference between OneDrive and the File Transfer Service?
A: Mr. Johnson: OneDrive for Business does have DLP, the File Transfer Service does not. File size is the same for both. OneDrive is more conducive to collaboration.

Action Item: Mr. Frohlich will insure that any updates made to DLP will be shared with the MT-ISAC.

Jon Straughn commented that he could send a social security number via Exchange without receiving a Tool Tip.
Mr. Johnson stated that it is possible to send the email faster than a tool tip can be generated. There have also been instances of the Tool Tip not working. SITSD is addressing this issue. Individuals not receiving Tool Tips on a regular basis should open a ticket with the Service Desk. Sensitive information sent via encrypted email will not trigger the Tool Tip. Mr. Johnson requested more live testers for DLP in Exchange. This will help ensure that the template is not generating false positives and blocking business practices.

Mr. Frohlich requested that the MT-ISAC approve giving access to the Enterprise Security Team to view the DLP reports located in the DLP mailbox. These reports contain the email subject and the template that was blocked. This will allow the Enterprise Security Team to identify false positives. There are over 4,000 emails currently in the DLP inbox. Mr. Frohlich would like his team to be able to spot check these emails to ensure that the template is blocking the correct information. Mr. Frohlich requested that the actual email be placed in the report allow staff to ensure that the templates are functioning correctly. This access would be terminated when DLP is turned on in live mode.

Q: Mr. Fuller: Who else on your team would have access to these emails?
A: Mr. Frohlich: Michael Barbere, Craig Marquardt and myself. It would be directed to Craig to go through the mailbox and spot check several times a week.
Mr. Fuller commented his concern about giving this authority Mr. Marquardt as a new hire and probationary employee.
Mr. Frohlich stated that this review could be performed by himself or Mr. Barbere.
Jon Straughn stated that he will need to have this request reviewed by the Department of Corrections (DOC) legal team due to the sensitive nature of the information involved.
Mr. Fuller and Ms. Kauska also stated that they would need more time to consider this request.
Q: Mr. Germaine: Do you have a way to filter these reports to identify repeat offenders?
A: Mr. Frohlich: There is not a way to search or filter these reports. The mailbox is very vague. We are working on a script to be able to sift through this mailbox.
Ms. Temple commented that Microsoft is aware of the issue with the DLP mailbox and is working on a solution.
Lynne Pizzini recommended that the council members discuss this request within their individual agencies prior to a vote.
Action Item: The request for authorizing Mr. Frohlich and Mr. Barbere to fully review DLP blocked emails will be added to the March 8, 2017 MT-ISAC agenda. *****UPDATE***** – Mr. Frohlich has withdrawn this request in February due to concerns from agencies, and will focus on DLP training and testing within agencies.

Channah Wells requested that agencies be allowed time, once the templates have been finalized, to review

what is being blocked before DLP goes live.

Action Item: Mr. Frohlich will work with Ms. Wells to ensure that DLP is not hindering business needs.

Q: Cyndie Lockett: How are you educating users about the adjustments made to the DLP templates?
A: Mr. Johnson: Changes made to the templates are completed through Change Requests. Notifications will be sent out concerning the changes made. These changes will also be discussed during the weekly NMG meeting.

Q: Ms. Lockett: Who is the correct contact for instances of DLP blocked information that is hindering a business need?
A: Mr. Johnson: Call extension 2000 and open a service desk ticket. Identify if the DLP issues are on OneDrive or Exchange and state the criticality of the business function.

Department of Homeland Security (DHS) Cyber Security Evaluation
Harley Rinerson gave a presentation on DHS Cyber Security Evaluations. This program is structured to support the protection of the Nation's Critical Infrastructure and Key Resources (CIKR) and State, Local, Territorial, and tribal (SLTT) governments. Program activities are currently focusing on Cyber Security Preparedness. Services provided by Mr. Rinerson include Cyber Resilience Review (CRR), Cyber Infrastructure Surveys (C-IST) and External Dependency Reviews (EDM). The Cyber Security Framework allows for the identification and protection from cyber security threats as well detection of possible threats and reduction of response time. A Cyber Resilience Review (CRR) is offered to states at no costs. The CRR will evaluate the maturity of a state's security program. There is a direct link between the NIST Cyber Security Framework and the Cyber Resilience Review. The CRR evaluates10 domains within a state security program to assess the maturity of the program. A Maturity Indicator Level (MIL) is then assigned which measures process institutionalization compared to similar organizations. This assessment allows states to identify points of cyber security weakness and areas that require improvement. The C-IST Survey is an assessment that focuses on 80 cyber security goals. The participating organization is then provided with a dashboard which allows them to run several different scenarios and identify areas of need. The EDM will assess state vendors and provide a view of vendor management and external dependencies of the participating organization. The Cyber Security Evaluation Tool (CSET) is a self-assessment tool for integrating cyber security into an existing risk management strategy. An ICS-CERT Architectural Review can also be performed to assess the security architecture for industrial control, process automation, and other cyber-physical systems. A Risk and Vulnerability Assessment (RVA) identifies risks and provides risk mitigation and remediation strategies. Cyber Hygiene assesses Internet accessible systems for known vulnerabilities and configuration errors.

Open Forum
Future Agenda Items
Action Item:

Public Comment
.
Action Item:

Next Meeting

Adjournment